SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Mihaela Laljek

LUCASOV TEOREM

Diplomski rad

Voditelj rada:
doc.dr.sc. Tomislav Pejković

Zagreb, rujan 2018.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Zahvaljujem se svom mentoru, doc. dr. sc. Tomislavu Pejkoviću na ukazanom povjerenju, pruženoj pomoći i podršci tijekom izrade diplomskog rada.

Od srca se zahvaljujem svojoj obitelji, dečku i prijateljima na strpljenju i velikoj podršci pruženoj tijekom studiranja.

Ovaj rad posvećujem svom djedu.

Sadržaj

Uvod

Teorija brojeva je sa svojih približno 4500 godina jedna od najstarijih grana matematike, a prvi tragovi mogu se pronaći kod Babilonaca još u drevnoj Mezopotamiji. Teorija brojeva naziva se i *kraljica matematike* zbog svog temeljnog položaja u matematici i velikog raspona područja kojeg obuhvaća. Ona prvenstveno proučava cijele brojeve, a zatim svojstva i osobine objekata koji su sačinjeni od njih. Tako se među predmetima proučavanja nalaze racionalni brojevi, prosti i složeni brojevi, algebarski brojevi i slično. Kroz svoju dugu povijest, teorija brojeva zaokupljala je umove mnogobrojnih velikih matematičara. Među njima se nalaze Pitagora, Euklid, Diofant, M. Mersenne, P. de Fermat, L. Euler, C. F. Gauss, te možda manje poznat, ali nikako manje važan Édouard Lucas.

François Édouard Anatole Lucas je francuski matematičar rođen 1842. godine u Amiensu. Školovao se na *École Normale Supérieure* u rodnom gradu, a obrazovanje nastavlja u Parizu gdje se kasnije zapošljava kao profesor matematike. Imao je reputaciju zabavnog i izazovnog profesora koji je često motivirao studente različitim matematičkim slagalicama. Još jedna zanimljivost vezana uz Lucasa jest da je upravo on osmislio mozgalicu koja je i danas vrlo popularna, a naziva se Hanojski tornjevi.

Najpoznatija Lucasova postignuća vezana su uz teoriju brojeva. Razvio je test kojim se provjerava je li neki prirodan broj n prost ili složen na temelju poznavanja prostih faktora od $n-1$. U literaturi test možemo pronaći pod imenom *Lucas-Lehmerov test prostosti*. Proučavao je Fibonaccijeve brojeve te je dao poznatu formulu za određivanje n-tog Fibonaccijevog broja

$$F_n = \frac{1}{\sqrt{5}} \cdot \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \cdot \left(\frac{1-\sqrt{5}}{2} \right)^n, n \in \mathbb{N}.$$

Fibonaccijeve brojeve možemo zadati rekurzivnom formulmom $F_n = F_{n-2}+F_{n-1}$ s početnim uvjetima $F_1 = 1$, $F_2 = 1$. Lucas je promatrao niz brojeva zadanih istom rekurzivnom formulom $L_n = L_{n-2} + L_{n-1}$ te početnim uvjetima $L_1 = 2, L_2 = 1$. Time se dobije niz brojeva $2, 1, 3, 4, 7, 11, 18, 29, 47...$ koji se u njegovu čast nazivaju Lucasovi brojevi. Također, Lucas je proučavao brojeve oblika $2^n - 1$, gdje je n prirodan broj, poznatije pod nazivom *Mersennovi brojevi.* Dokazao je kako je broj $2^{127} - 1$ prost broj, a to je ujedno najveći Mersennov prost broj pronađen bez pomoći računala.

Ovaj diplomski rad posvećen je Lucasovom teoremu koji je od važnosti za teoriju brojeva, a pomoću njega možemo na lak način ustanoviti vrijednost binomnog koeficijenta modulo prost broj. Teorem je opisao 1878. godine u svom članku *Théorie des Fonctions Numériques Simplement Périodiques* objavljenom u časopisu *American Journal of Mathematics*.

U prvom poglavlju navedeni su temeljni pojmovi potrebni za razumijevanje daljnjeg rada, te tvrdnje koje se upotrebljavaju u kasnijim dokazima. U idućem poglavlju naveden je iskaz Lucasovog teorema koji je zatim dokazan na dva različita načina. Prvo se radi o algebarskom, a nakon njega o kombinatornom dokazu. U sljedećem poglavlju navedene su neke od primjena Lucasovog teorema, od kojih je jedna i karakterizacija prostih brojeva. Na kraju ovog rada dane su generalizacije Lucasovog teorema. Prve dvije generalizacije posvećene su vrijednosti binomnog koeficijenta modulo p^3, gdje je p prost broj, dok je na kraju obrađena Kazandzidisova generalizacija Lucasovog teorema.

Diplomski rad napravljen je u sklopu aktivnosti Projekta KK.01.1.1.01.0004 - Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri.

Poglavlje 1

Osnovni pojmovi i tvrdnje

Na samom početku ovog rada navedeni su osnovni pojmovi, definicije i teoremi potrebni za razumijevanje i dokazivanje tvrdnji u nastavku.

Definicija 1.1. *Neka su a i b cijeli brojevi, pri čemu je $a \neq 0$. Kažemo da je b djeljiv s a, odnosno a dijeli b, ako postoji cijeli broj k takav da je $b = ka$. Pritom koristimo oznaku $a \mid b$. Ako a ne dijeli b, onda pišemo $a \nmid b$.*
Oznaka $a^x \parallel b$ znači da $a^x \mid b$, ali $a^{x+1} \nmid b$.

Definicija 1.2. *Neka su a, b i c cijeli brojevi. Broj a nazivamo zajednički djelitelj od b i c ako $a \mid b$ i $a \mid c$. Ako je barem jedan od brojeva b i c različit od nule, onda postoji konačno mnogo djelitelja od b i c. Najveći od njih naziva se najveći zajednički djelitelj brojeva b i c i označava se s (b, c).*

Teorem 1.3. *Brojevi $\dfrac{a}{(a,b)}$ i $\dfrac{b}{(a,b)}$ su relativno prosti.*

Dokaz. Neka je $d = (a, b)$ najveći zajednički djelitelj brojeva a i b. Neka je $a_1 = a/d$ i $b_1 = b/d$. Pretpostavimo suprotno, to jest a_1 i b_1 nisu relativno prosti brojevi. Označimo tada s $d_1 > 1$ njihovog najvećeg zajedničkog djelitelja, to jest $d_1 = (a_1, b_1)$. U tom slučaju su $a_2 = a_1/d_1$ i $b_2 = b_1/d_1$ cijeli brojevi. Sada smo dobili jednakosti $a = dd_1a_2$ i $b = dd_1b_2$ iz kojih vidimo da je dd_1 zajednički djelitelj od a i b. Ranije smo definirali d kao najveći zajednički djelitelj od a i b, pa slijedi $dd_1 < d$. Znamo da je $d_1 > 1$, pa $dd_1 < d$ nije moguće. Time smo došli do kontradikcije. Prema tome, zaključujemo da su a_1 i b_1 relativno prosti brojevi čime je dokazana tvrdnja teorema. □

Teorem 1.4 (**Teorem o dijeljenju s ostatkom**). *Za proizvoljni cijeli broj m i prirodni broj n postoje jedinstveni cijeli brojevi k i r, $0 \leq r < n$, takvi da je*

$$m = k \cdot n + r.$$

Broj k nazivamo kvocijent ili količnik, a broj r ostatak pri dijeljenju.

Dokaz. Dokaz možete pronaći u [3] na stranici 2. □

Teorem 1.5. *Za cijele brojeve a i b koji nisu oba jednaka nuli, postoje cijeli brojevi u i v takvi da je* $(a, b) = ua + vb$.

Dokaz. Dokaz možete pronaći u [3] na stranici 3. □

Koristeći teorem o dijeljenju s ostatkom možemo svaki prirodan broj prikazati u zadanoj bazi.

Teorem 1.6 (**Prikaz broja u bazi**). *Neka je* $b \geq 2$ *zadani prirodan broj. Za svaki prirodan broj n postoji jedinstven niz znamenaka* $(x_k, \ldots, x_1, x_0)$, $x_i \in \{0, 1, \ldots, b-1\}$, $x_k \neq 0$, *takav da je*

$$n = x_k \cdot b^k + x_{k-1} \cdot b^{k-1} + \cdots + x_1 \cdot b + x_0.$$

Ovaj zapis nazivamo zapis broja n u bazi b.

Dokaz. Prvo dokazujemo egzistenciju prikaza broja n u bazi b. Uvodimo oznaku $n_0 = n$, a zatim podijelimo n_0 s b. Prema teoremu 1.4 postoji jedinstveni kvocijent n_1 i ostatak x_0 takvi da je

$$n_0 = n_1 \cdot b + x_0.$$

Sada podijelimo n_1 s b pa dobivamo

$$n_1 = n_2 \cdot b + x_1.$$

Analogno nastavljamo postupak. Svaki sljedeći n_i dobivamo kada prethodni cjelobrojno dijelimo s $b \geq 2$. Jasno je da ćemo nakon konačno mnogo koraka doći do kvocijenta 0. U posljednjem koraku imamo

$$n_k = 0 \cdot b + x_k.$$

Kada bismo nastavili postupak, svi daljni kvocijenti i ostaci bili bi jednaki 0. Navedeni postupak staje nakon konačno mnogo koraka.

Za sve ostatke $x_i, 0 \leq i \leq k$ vrijedi $0 \leq x_i \leq b-1$. Pretpostavimo da nam je bilo potrebno k koraka da dobijemo kvocijent $n_{k+1} = 0$. Sada redom uvršavajući n_k u n_{k-1}, zatim n_{k-1} u n_{k-2} i tako dalje, dobivamo

$$\begin{aligned} n_k &= x_k \\ n_{k-1} &= x_k \cdot b + x_{k-1} \\ &\vdots \\ n_1 &= x_k \cdot b^{k-1} + \cdots + x_1 \end{aligned}$$

$$n_0 = n_1 \cdot b + x_0 = x_k \cdot b^k + \cdots + x_1 \cdot b + x_0.$$

Vidimo da je

$$n = n_0 = x_k \cdot b^k + \cdots + x_1 \cdot b + x_0 \tag{1.1}$$

te smo time dokazali egzistenciju prikaza broja n u bazi b.

Dokažimo sada jedinstvenost tog prikaza. Pretpostavimo da uz (1.1) postoji još jedan prikaz

$$n = y_l \cdot b^l + \cdots + y_1 \cdot b + y_0.$$

Tada je

$$n = (x_k \cdot b^{k-1} + \cdots + x_1) \cdot b + x_0 = (y_l \cdot b^{l-1} + \cdots + y_1) \cdot b + y_0$$

iz čega dobivamo $x_0 \equiv y_0 \equiv n \pmod{b}$, te je zbog $x_0, y_0 \in \{0, 1, \ldots, b-1\}$ nužno $x_0 = y_0$. Slijedi

$$x_k \cdot b^{k-1} + \cdots + x_2 \cdot b + x_1 = \frac{n - x_0}{b} = \frac{n - y_0}{b} = y_l \cdot b^{l-1} + \cdots + y_2 \cdot b + y_1.$$

Analogno nastavimo postupak čime dobivamo $k = l$ te tvrdnju da su sve znamenke na odgovarajućim mjestima jednake. □

Zapis broja u bazi b uvijek možemo nadopuniti s nulama na vodećim mjestima i pritom se vrijednost broja neće promijeniti.

Definicija 1.7. *Prirodan broj p veći od 1 koji je djeljiv samo s 1 i samim sobom nazivamo prost broj. Ako prirodan broj veći od 1 nije prost, onda kažemo da je složen broj.*

Teorem 1.8. *Ako je p prost broj i p dijeli umnožak ab, onda p dijeli a ili p dijeli b.*

Dokaz. Neka je p prost broj takav da p dijeli umnožak ab. Pretpostavimo da p ne dijeli a. Preostaje nam dokazati da u tom slučaju p dijeli b. Tvrdnja $p \mid ab$ povlači da postoji cijeli broj k takav da je $ab = pk$. Jedini djelitelji od p su ± 1 i $\pm p$, a kako $p \nmid a$ slijedi da je $(a, p) = 1$. Tada postoje cijeli brojevi x i y takvi da je $xa + yp = 1$. Sada imamo

$$\begin{aligned} b &= b \cdot 1 = b \cdot (xa + yp) \\ &= b(xa) + b(yp) = x(ab) + b(yp) \\ &= x(kp) + (by)p = p(xk + by) \end{aligned}$$

iz čega vidimo da je b djeljiv s p. Uz pretpostavku da p ne dijeli b, analognim postupkom bismo pokazali da tada p dijeli a. □

Pojam kongruencije prvi je upotrijebio C.F. Gauss u svom djelu *Disquisitiones Arithmeticae* 1801. godine. U nastavku je navedena definicija kongruencija te su dokazana neka od svojstava koja koristimo u ovom radu.

Definicija 1.9. *Neka su a i b cijeli brojevi. Ako cijeli broj m različit od nule dijeli razliku $a-b$, onda kažemo da je a kongruentan b modulo m i pišemo $a \equiv b \pmod{m}$. U protivnom, kažemo da a nije kongruentan b modulo m i pišemo $a \not\equiv b \pmod{m}$.*

Teorem 1.10. *Relacija "biti kongruentan modulo m" je relacija ekvivalencije na skupu cijelih brojeva.*

Dokaz. Kako bismo dokazali da je to relacija ekvivalencije, potrebno je dokazati da vrijede svojstva refleksivnosti, simetričnosti i tranzitivnosti.

a) Znamo da $m \mid 0$, to jest $m \mid (a - a)$, pa vrijedi tvrdnja $a \equiv a \pmod{m}$.

b) Ako vrijedi $a \equiv b \pmod{m}$, onda postoji cijeli broj k takav da je $a - b = mk$. Navedenu jednakost pomnožimo s -1 pa dobivamo $b - a = m(-k)$. Slijedi tvrdnja $b \equiv a \pmod{m}$.

c) Ako je $a \equiv b \pmod{m}$ i $b \equiv c \pmod{m}$, onda postoje cijeli brojevi k i l takvi da je $a - b = mk$ i $b - c = ml$. Zbrajanjem ovih dviju jednakosti dobivamo $a - b + b - c = mk + ml$, odnosno $a - c = m(k + l)$. Iz navedene jednakosti slijedi $a \equiv c \pmod{m}$.

□

Teorem 1.11. *Neka su a, b, c i d cijeli brojevi. Ako je $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, onda vrijedi*

a) $a + c \equiv b + d \pmod{m}$

Dokaz. Neka je $a - b = mk$ i $c - d = ml$. Zbrajanjem ovih dviju jednakosti dobivamo $a - b + c - d = mk + ml$, odnosno $(a + c) - (b + d) = m(k + l)$ čime smo pokazali da vrijedi navedena tvrdnja. □

b) $a - c \equiv b - d \pmod{m}$

Dokaz. Neka je $a - b = mk$ i $c - d = ml$. Oduzimanjem ovih dviju jednakosti dobivamo $a - b - c + d = mk - ml$, odnosno $(a - c) - (b - d) = m(k - l)$ čime smo pokazali da vrijedi navedena tvrdnja. □

c) $ac \equiv bd \pmod{m}$

Dokaz. Neka je $a - b = mk$ i $c - d = ml$. Vrijedi

$$ac - bd = a(c - d) + d(a - b) = a(ml) + d(mk) = m(al + dk)$$

odakle slijedi navedena tvrdnja. □

Teorem 1.12. *Neka su a, b i d cijeli brojevi. Ako je $a \equiv b \pmod{m}$ i $d \mid m$, onda je $a \equiv b \pmod{d}$.*

Dokaz. Iz $a \equiv b \pmod{m}$ slijedi $a - b = mk$. Neka je $m = de$. Tada je $a - b = d(ek)$, pa je $a \equiv b \pmod{d}$. □

Teorem 1.13. *Neka su a, b i c cijeli brojevi, pri čemu je $c \neq 0$. Ako je $a \equiv b \pmod{m}$, onda je $ac \equiv bc \pmod{mc}$.*

Dokaz. Iz $a \equiv b \pmod{m}$ slijedi $a - b = mk$. Ako navedenu jednakost pomnožimo s c, dobivamo $ac - bc = (mc)k$, pa je $ac \equiv bc \pmod{mc}$. □

Teorem 1.14. *Tvrdnja $ax \equiv ay \pmod{m}$ vrijedi ako i samo ako je $x \equiv y \pmod{\frac{m}{(a,m)}}$. Posebno, ako je $ax \equiv ay \pmod{m}$ i $(a, m) = 1$, onda je $x \equiv y \pmod{m}$.*

Dokaz. Ako je $ax \equiv ay \pmod{m}$, onda postoji cijeli broj z takav da je $ax - ay = mz$, odnosno $a(x - y) = mz$. Podijelimo izraz s najvećim zajedničkim djeliteljem od a i m, pa dobivamo

$$\frac{a}{(a,m)}(x - y) = \frac{m}{(a,m)}z$$

iz čega slijedi da $\frac{m}{(a,m)}$ dijeli $\frac{a}{(a,m)}(x - y)$. Prema teoremu 1.3 znamo da su brojevi $\frac{m}{(a,m)}$ i $\frac{a}{(a,m)}$ relativno prosti, pa zaključujemo da $\frac{m}{(a,m)}$ dijeli $x - y$, to jest

$$x \equiv y \pmod{\frac{m}{(a,m)}}.$$

U drugom smjeru, pretpostavimo da vrijedi $x \equiv y \pmod{\frac{m}{(a,m)}}$. Tada prema teoremu 1.13 vrijedi $ax \equiv ay \pmod{\frac{am}{(a,m)}}$. Uočimo kako je m djelitelj od $\frac{am}{(a,m)}$ pa primjenom teorema 1.12 dobivamo $ax \equiv ay \pmod{m}$. □

Teorem 1.15 (**Wilsonov teorem**). *Prirodan broj p veći od 1 je prost ako i samo ako je*

$$(p - 1)! \equiv -1 \pmod{p}.$$

Dokaz. Dokaz možete pronaći u [9] na stranici 549. □

Definicija 1.16. *Umnožak prvih n prirodnih brojeva označavamo s $n!$, to jest $1 \cdot 2 \cdots n = n!$. Taj broj nazivamo n faktorijela. Dodatno definiramo $0! = 1$.*

Definicija 1.17. *Neka su m i n nenegativni cijeli brojevi. Broj svih n-članih podskupova m-članog skupa bilježimo simbolom $\binom{m}{n}$ i nazivamo ga binomni koeficijent. Pri tome vrijedi*

$$\binom{m}{n} = \frac{m(m-1)(m-2)\cdots(m-n+1)}{n(n-1)\cdots 1},$$

odnosno za $m \geq n$

$$\binom{m}{n} = \frac{m!}{n!(m-n)!}.$$

Ako je $m < n$, onda je $\binom{m}{n} = 0$. Vidimo i da je $\binom{m}{0} = 1$.

Teorem 1.18 (**Binomni teorem**). *Za svaki nenegativni cijeli broj m i realne brojeve x i y vrijedi*

$$(x+y)^m = x^m + \binom{m}{1}x^{m-1}y + \cdots + \binom{m}{n}x^n y^{m-n} + \cdots + \binom{m}{m-1}xy^{m-1} + y^m = \sum_{n=0}^{m}\binom{m}{n}x^n y^{m-n}.$$

Dokaz. Dokaz možete pronaći u [11] na stranicama 78 – 79. □

Binomni koeficijent $\binom{m}{n}$ možemo definirati i ako m nije prirodan broj te ga tada nazivamo opći binomni koeficijent. U tom slučaju kombinatorna interpretacija nema smisla.

Definicija 1.19. *Za realan (ili kompleksan) broj m i nenegativan cijeli broj n, opći binomni koeficijent $\binom{m}{n}$ definira se kao*

$$\binom{m}{n} = \frac{m(m-1)\cdots(m-n+1)}{n(n-1)\cdots 1}.$$

Vrijedi i sljedeća generalizacija binomnog teorema koja govori o razvoju odgovarajuće funkcije u Taylorov red oko 0. Pri tome ove redove potencija promatramo samo kao formalne redove, to jest ne zanima nas gdje konvergiraju. Lako se pokazuje da vrijedi

$$\binom{m}{n} = (-1)^n\binom{-m+n-1}{n}.$$

Teorem 1.20 (**Binomni red**). *Za sve cijele brojeve z, $|z| < 1$ i za sve realne brojeve a vrijedi*

$$(1+z)^a = \sum_{k=0}^{\infty}\binom{a}{k}z^k = 1 + \binom{a}{1}z + \binom{a}{2}z^2 + \binom{a}{3}z^3 + \cdots$$

Primjerice, vrijede ovi razvoji u redove potencija:

$$\frac{1}{1-z} = (1-z)^{-1} = \sum_{k=0}^{\infty}\binom{-1}{k}(-z)^k = \sum_{k=0}^{\infty}(-1)^k\binom{1+k-1}{k}(-z)^k = \sum_{k=0}^{\infty}z^k;$$

$$\frac{1}{(1-z)^{n+1}} = \sum_{k=0}^{\infty}\binom{-n-1}{k}(-z)^k = \sum_{k=0}^{\infty}\binom{n+k}{k}z^k, n \in \mathbb{N};$$

$$\frac{1}{(1-z)^2} = \sum_{k=0}^{\infty}\binom{k+1}{k}z^k = \sum_{k=0}^{\infty}(k+1)z^k.$$

Poglavlje 2

Lucasov teorem

Mnogi matematičari 19. stoljeća proučavali su ostatke pri dijeljenju binomnog koeficijenta s potencijama prostih brojeva. Među njima su C. Babbage, A. L. Cauchy, A. Cayley, C. F. Gauss, K. Hensel, C. Hermite, E. Kummer, A. M. Legendre, E. Lucas i L. Stickelberger. U ovom radu posvetit ćemo se Lucasovom teoremu. Kao što je već navedeno, teorem je objavljen u Lucasovom djelu *Théorie des fonctions numériques simplement périodiques*, a omogućuje nam jednostavno određivanje vrijednosti binomnog koeficijenta modulo prost broj.

U ovom poglavlju ćemo iskazati Lucasov teorem, a zatim slijede dva razlčita dokaza. Na kraju se nalazi primjer u kojemu je prikazana njegova direktna primjena kod računanja ostatka prilikom dijeljenja binomnog koeficijenta s prostim brojem. Prije samog iskaza, navesti ćemo dvije tvrdnje koje ćemo koristiti u dokazu teorema.

Lema 2.1. *Neka je p prost broj. Tada za svaki $k \in \{1, 2, \ldots, p-1\}$ vrijedi*

$$\binom{p}{k} \equiv 0 \pmod{p}.$$

Dokaz. Prema definiciji 1.17 imamo $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. Kako je p prost broj, $k \in \{1, 2, \ldots, p-1\}$, a prema tome i $(p-k) \in \{1, 2, \ldots, p-1\}$, uočimo da nazivnik $k!(p-k)!$ nije djeljiv s p. S druge strane, brojnik $p!$ je djeljiv s p, pa je prema tome i $\binom{p}{k}$ djeljivo s p, odnosno vrijedi tvrdnja leme. □

Lema 2.2. *Za svaki realan broj x i nenegativni cijeli broj r, te prost broj p vrijedi*

$$(1+x)^{p^r} \equiv 1 + x^{p^r} \pmod{p}.$$

Dokaz. Dokaz ćemo provesti koristeći princip matematičke indukcije.
Za $r = 0$ imamo

$$1 + x \equiv 1 + x \pmod{p},$$

pa tvrdnja očito vrijedi. Provjerimo vrijedi li tvrdnja za $r = 1$. Prema teoremu 1.18 imamo

$$\begin{aligned}(1+x)^p &= \binom{p}{0}1^p x^0 + \binom{p}{1}1^{p-1}x^1 + \cdots + \binom{p}{p-1}1^1 x^{p-1} + \binom{p}{p}1^0 x^p \\ &= 1 + \binom{p}{1}x + \cdots + \binom{p}{p-1}x^{p-1} + x^p.\end{aligned}$$

Primjenimo li lemu 2.1, uočavamo da su svi binomni koeficijenti u zadnjem redu djeljivi s p, odnosno vrijedi

$$(1+x)^p \equiv 1 + x^p \pmod{p}.$$

Time smo pokazali da tvrdnja vrijedi za $r = 1$. Pretpostavimo da tvrdnja

$$(1+x)^{p^r} \equiv 1 + x^{p^r} \pmod{p}$$

vrijedi za neki prirodan broj r. Provjerimo vrijedi li tvrdnja tada i za $r + 1$.

$$\begin{aligned}(1+x)^{p^{r+1}} &= (1+x)^{p^r \cdot p} \\ &= \left((1+x)^{p^r}\right)^p \\ &\equiv (1 + x^{p^r})^p \\ &\equiv 1 + x^{p^r \cdot p} \\ &\equiv 1 + x^{p^{r+1}} \pmod{p}\end{aligned}$$

Koristeći pretpostavku i dokazanu tvrdnju za $r = 1$, pokazali smo da tvrdnja vrijedi za $r + 1$, pa prema principu matematičke indukcije zaključujemo da tvrdnja leme vrijedi za sve nenegativne cijele brojeve r. □

Slijedi iskaz i algebarski dokaz Lucasovog teorema naveden u članku [4].

Teorem 2.3 (**Lucasov teorem**). *Neka su m i n nenegativni cijeli brojevi, a p prost broj. Ako su*

$$\begin{aligned}m &= m_k p^k + m_{k-1}p^{k-1} + \cdots + m_1 p + m_0 \quad i \\ n &= n_k p^k + n_{k-1}p^{k-1} + \cdots + n_1 p + n_0\end{aligned}$$

zapisi brojeva m i n u bazi p, onda je

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \pmod{p}.$$

Dokaz. Korištenjem teorema 1.18, zapisa broja m u bazi p te leme 2.2 dobivamo

$$\begin{aligned}
\sum_{N=0}^{m} \binom{m}{N} x^N &= (1+x)^m \\
&= (1+x)^{m_k p^k + m_{k-1} p^{k-1} + \cdots + m_1 p + m_0} \\
&= \prod_{i=0}^{k} (1+x)^{m_i p^i} \\
&= \prod_{i=0}^{k} \left((1+x)^{p^i}\right)^{m_i} \\
&\equiv \prod_{i=0}^{k} \left(1+x^{p^i}\right)^{m_i} \pmod{p} \\
&= \prod_{i=0}^{k} \left(\sum_{s_i=0}^{m_i} \binom{m_i}{s_i} \left(x^{p^i}\right)^{s_i} \right) \\
&= \prod_{i=0}^{k} \left(\sum_{s_i=0}^{m_i} \binom{m_i}{s_i} x^{s_i p^i} \right) \qquad (2.1)
\end{aligned}$$

Zapišimo jednakost 2.1 tako da grupiramo koeficijente uz pojedinu potenciju od x. Time dobivamo izraz

$$\sum_{N=0}^{m} \left(\sum \prod_{i=0}^{k} \binom{m_i}{s_i} \right) x^N,$$

pri čemu smo unutarnju sumu uzeli po skupovima $(s_0, s_1, \ldots, s_k)$ takvim da je $\sum_{i=0}^{k} s_i p^i = N$. Kako je $0 \leq s_i \leq m_i \leq p-1$, tada je $\sum_{i=0}^{k} s_i p^i = N$ prikaz broja N u bazi p, a takav prikaz je prema teoremu 1.6 jedinstven. Prema tome, izjednačimo li za $n \leq m$ koeficijente uz x^n dobivamo tvrdnju teorema, odnosno

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \pmod{p}.$$

Primijetimo da za $n > m$ vrijedi $\binom{m}{n} = 0$, a za barem jedan i je $n_i > m_i$ jer bi u protivnom bilo $n \leq m$ te je $\prod_{i=0}^{k} \binom{m_i}{n_i} = 0$. Zato tvrdnja Lucasovog teorema vrijedi i u tom slučaju. □

Postoji više dokaza Lucasovog teorema u kojima se koriste različite metode dokazivanja. U nastavku ćemo navesti kombinatorni dokaz iz članka [6], ali prije samog dokaza potrebna nam je sljedeća tvrdnja. Broj elemenata skupa X označavat ćemo sa $|X|$.

Lema 2.4. *Neka je X konačan skup, a p prost broj. Neka je $f : X \to X$ funkcija takva da je $f^p = f \circ f \circ \cdots \circ f = id$ identiteta. Označimo s X_0 skup fiksnih točaka funkcije f, $X_0 = \{x \in X \mid f(x) = x\}$. Tada je*

$$|X| \equiv |X_0| \pmod{p}.$$

Dokaz. Za svaki $x \in X$ definiramo orbitu $\bar{x}$ od x kao skup $\left\{x, f(x), \ldots, f^{p-1}(x)\right\}$. Orbite particioniraju skup X. Očito je $|\bar{x}| = 1$ ako i samo ako je $x = f(x)$, odnosno ako je x iz skupa fiksnih točaka X_0. Sada tvrdimo da iz $|\bar{x}| > 1$, slijedi $|\bar{x}| = p$. Ako su svi elementi u orbiti međusobno različiti, tvrdnja očito vrijedi. Ako u $\bar{x}$ postoji element koji se ponavlja, tada za neke $0 \leq i < j < p$ vrijedi $f^i(x) = f^j(x)$. Na jednakost $f^i(x) = f^j(x)$ djelujemo sa f^{-1} točno i puta te tako dobivamo $f^{j-i}(x) = x$. Znamo da je $f^p(x) = x$. Najveći zajednički djelitelj od $j - i$ i p je 1 jer je p prost broj. Zato prema teoremu 1.5 postoje cijeli brojevi a i b takvi da je $a(j - i) + bp = 1$ pa imamo

$$f(x) = f^{a(j-i)+bp}(x) = f^{a(j-i)}\left(f^{bp}(x)\right) = f^{a(j-i)}(x) = x.$$

Dakle, $|\bar{x}| = 1$. Time smo dokazali da iz $|\bar{x}| > 1$, slijedi $|\bar{x}| = p$.

Ukupno imamo $|X_0|$ fiksnih točaka, odnosno $|X_0|$ orbita duljine 1 te preostalih $n \in \mathbb{N}$ orbita duljina p, pa prema tome vrijedi

$$|X| = |X_0| + np.$$

Iz dobivene jednakosti slijedi kongruencija

$$|X| \equiv |X_0| \pmod{p}.$$

□

Dokažimo sada Lucasov rezultat pomoću teorema 2.4.

Dokaz. Zapišimo m i n u obliku $m = Mp + m_0$ i $n = Np + n_0$. U tom slučaju, dovoljno je pokazati

$$\binom{m}{n} \equiv \binom{M}{N}\binom{m_0}{n_0} \pmod{p}$$

jer se uzastopnom primjenom takve jednakosti dobiva tvrdnja teorema 2.3.

Za početak definiramo skupove

$$A_i = \{(i, 1), (i, 2), \ldots, (i, M)\} \quad 1 \leq i \leq p,$$
$$B = \{(0, 1), (0, 2), \ldots, (0, m_0)\},$$

a zatim

$$A = A_1 \cup A_2 \cup \ldots \cup A_p \cup B.$$

Iz konstrukcije skupa A vrijedi

$$|A| = Mp + m_0 = m.$$

Sada definiramo funkciju $f : A \to A$ koja ciklički pomiče skupove A_i, a fiksira B, to jest

$$\begin{aligned} f(i, x) &= (i + 1, x), \quad 1 \leq i \leq p - 1, \\ f(p, x) &= (1, x), \\ f(0, x) &= (0, x). \end{aligned}$$

Prema tome, vrijedi

$$\begin{aligned} f(A_i) &= A_{i+1}, \quad 1 \leq i \leq p - 1, \\ f(A_p) &= A_1, \\ f(B) &= B. \end{aligned}$$

Funkcija f zadovoljava svojstvo iz leme 2.4 jer je očito $f^p = id$.

Za skup X uzet ćemo familiju svih skupova $C \subseteq A$ za koje vrijedi $|C| = n$. Budući je $f : A \to A$, f djeluje prirodno na podskupove od A, $f(C) = \{f(x)|x \in C\}$. Funkcija f je bijekcija, pa je $|f(C)| = |C|$ te je $f : X \to X$, $f^p = id$. Očito je

$$|X| = \binom{m}{n}.$$

Nakon što smo odredili kardinalni broj skupa X, preostaje nam odrediti broj elemenata u skupu fiksnih točaka X_0. Svaki podskup C skupa A možemo na jedinstven način zapisati kao

$$C = C_1 \cup C_2 \cup \ldots \cup C_p \cup C_0,$$

pri čemu je $C_i \subseteq A_i$, a $C_0 \subseteq B$. Funkcija f ciklički pomiče skupove A_i te fiksira skup B, pa je $f(C) = C$ ako i samo ako vrijedi

$$C_i = f^{i-1}(C_1), \quad 1 \leq i \leq p.$$

Za $C \in X$ vrijedi $|C| = n$, a za $C \in X_0$ imamo

$$|C| = p|C_1| + |C_0| = n = Np + n_0.$$

Kako za $|C_0|$ i n_0 vrijedi $0 \leq |C_0| < p$ i $0 \leq n_0 < p$, vidimo da je $|C_0| = n_0$. Iz dobivene tvrdnje slijedi $|C_1| = N$.

Imamo n_0 elemenata skupa C_0, a biramo ih od ukupno m_0 elemenata koliko ih se nalazi u skupu B. Prema tome, elemente skupa C_0 možemo odabrati na $\binom{m_0}{n_0}$ načina. U skupu C_1

nalazi se N elemenata koje biramo od ukupno M elemenata iz skupa A_1. Znači, elemente skupa C_1 možemo odabrati na $\binom{M}{N}$ načina čime su određeni i elementi preostalih skupova. Primijenimo li pravilo produkta, dobivamo

$$|X_0| = \binom{M}{N}\binom{n_0}{m_0}.$$

Prema lemi 2.4 vrijedi $|X| \equiv |X_0| \pmod{p}$, odnosno u našem slučaju

$$\binom{m}{n} \equiv \binom{M}{N}\binom{m_0}{n_0} \pmod{p}.$$

□

Prije nego što se posvetimo posljedicama Lucasovog teorema, pogledajmo na idućem primjeru direktnu primjenu Lucasovog teorema kod računanja ostatka prilikom dijeljenja binomnog koeficijenta s prostim brojem.

Primjer 2.5. *Odredite ostatak pri dijeljenju* $\binom{1000}{200}$ *s* 13.

Kako bismo mogli primijeniti Lucasov teorem, prvo moramo prikazati brojeve 1000 i 200 u bazi 13:

$$1000 = 5 \cdot 13^2 + 11 \cdot 13 + 12,$$
$$200 = 1 \cdot 13^2 + 2 \cdot 13 + 5.$$

Primjenom Lucasovog teorema 2.3 dobivamo:

$$\begin{aligned}\binom{1000}{200} &\equiv \binom{5}{1}\binom{11}{2}\binom{12}{5} \\ &\equiv 5 \cdot 55 \cdot 792 \\ &\equiv 11 \pmod{13}.\end{aligned}$$

Prema tome, ostatak pri dijeljenju $\binom{1000}{200}$ s 13 je 11.

Poglavlje 3

Neke primjene Lucasovog teorema

U ovom poglavlju razrađene su neke od primjena Lucasovog teorema, navedene u člancima [2] i [4].

Teorem 3.1. *Neka je p prost, a m i n nenegativni cijeli brojevi čiji zapisi u bazi p glase*

$$m = m_k p^k + m_{k-1} p^{k-1} + \cdots + m_1 p + m_0 \quad i$$

$$n = n_k p^k + n_{k-1} p^{k-1} + \cdots + n_1 p + n_0.$$

Binomni koeficijent $\binom{m}{n}$ djeljiv je s p ako i samo ako za barem jedan par znamenaka n_i i m_i, $0 \leq i \leq k$ vrijedi $n_i > m_i$.

Dokaz. Pretpostavimo da je binomni koeficijent $\binom{m}{n}$ djeljiv s p. Prema definiciji 1.9 navedenu tvrdnju možemo zapisati kao

$$\binom{m}{n} \equiv 0 \pmod{p}.$$

Prema Lucasovom teoremu 2.3 imamo

$$\binom{m}{n} \equiv \prod_{j=0}^{k} \binom{m_j}{n_j} \pmod{p}.$$

Iz navedenih tvrdnji slijedi da je za barem jedan i

$$\binom{m_i}{n_i} \equiv 0 \pmod{p}.$$

Za $m_i \geq n_i$ je zbog $0 \leq n_i$ te $m_i < p$ i definicije binomnog koeficijenta očito da $p \nmid \binom{m_i}{n_i}$. Zaključujemo da je nužno $m_i < n_i$.

U drugom smjeru, pretpostavimo da za barem jedan par znamenaka n_i, m_i, $0 \leq i \leq k$ vrijedi $n_i > m_i$. Tada je $\binom{m_i}{n_i} = 0$, pa je

$$\prod_{j=0}^{k} \binom{m_j}{n_j} = 0,$$

te prema Lucasovom teoremu 2.3 slijedi

$$\binom{m}{n} \equiv 0 \pmod{p},$$

odnosno binomni koeficijent $\binom{m}{n}$ je djeljiv s p. □

Teorem 3.2. *Neka je p prost broj, a m nenegativni cijeli broj čiji zapis u bazi p glasi*

$$m = m_k p^k + m_{k-1} p^{k-1} + \cdots + m_1 p + m_0.$$

Neka je $T(m)$ broj cijelih brojeva n za koje vrijedi $0 \leq n \leq m$ i $\binom{m}{n} \not\equiv 0 \pmod{p}$. Tada je

$$T(m) = \prod_{i=0}^{k} (m_i + 1).$$

Dokaz. Neka je n cijeli broj takav da je $0 \leq n \leq m$ i neka je $n = n_k p^k + n_{k-1} p^{k-1} + \cdots + n_1 p + n_0$ njegov zapis u bazi p. Prema Lucasovom teoremu 2.3 vrijedi

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \pmod{p}.$$

Početna tvrdnja $\binom{m}{n} \not\equiv 0 \pmod{p}$ ekvivalentna je

$$\binom{m_i}{n_i} \not\equiv 0 \pmod{p}, \quad 0 \leq i \leq k.$$

Kako je $m_i < p$, svaki n_i biramo iz skupa $\{0, 1, \ldots, m_i\}$. Primijenimo li princip produkta, dobivamo tvrdnju teorema

$$T(m) = \prod_{i=0}^{k} (m_i + 1).$$

□

Teorem 3.3. *Neka je p prost broj i m prirodan broj. Nužan i dovoljan uvjet da svi binomni koeficijenti $\binom{m}{n}$, $0 < n < m$, budu djeljivi s p jest da m bude potencija broja p.*

Dokaz. Za $n = 0$ i $n = m$ je

$$\binom{m}{n} = 1 \not\equiv 0 \pmod{p}$$

pa je $T(m) \geq 2$. Tvrdnja teorema ekvivalentna je tvrdnji $T(m) = 2$, a prema prethodnom teoremu to vrijedi ako i samo ako je točno jedna od znamenaka u zapisu broja m u bazi p jednaka 1, a sve ostale znamenke su 0, odnosno u bazi p broj m ima zapis $10\ldots0$. Broj m ima navedeni zapis u bazi p ako i samo ako je m potencija broja p. □

Teorem 3.4. *Neka je $m = m_k p^k + m_{k-1}p^{k-1} + \cdots + m_1 p + m_0$, gdje je $m_k \neq 0$, zapis broja m u bazi p pri čemu je p prost broj. Nužan i dovoljan uvjet da niti jedan binomni koeficijent $\binom{m}{n}$, gdje je $0 \leq n \leq m$, nije djeljiv s p jest da vrijedi $m_i = p - 1$, $0 \leq i \leq k - 1$.*

Dokaz. Neka je $m^* = m - m_k p^k$. Pretpostavimo da vrijedi $T(m) = m + 1$. Primjenom teorema 3.2, imamo

$$\begin{aligned} m_k p^k + m^* + 1 = m + 1 &= T(m) \\ &= (m_k + 1)T(m^*) \\ &\leq (m_k + 1)(m^* + 1) \\ &= m_k(m^* + 1) + m^* + 1 \\ &\leq m_k p^k + m^* + 1. \end{aligned}$$

Prva i posljednja vrijednost su jednake, pa prema tome vrijedi $m^* = p^k - 1$. U drugom smjeru, pretpostavimo da je $m^* = p^k - 1$. Tada imamo

$$\begin{aligned} T(m) &= (m_k + 1)p^k \\ &= m_k p^k + m^* + 1 \\ &= m + 1. \end{aligned}$$

□

U duhu Lucasovog teorema dobivamo sljedeću karakterizaciju prostih brojeva. U nastavku koristimo oznaku $\lfloor x \rfloor$ kojom označavamo najveći cijeli broj manji ili jednak realnom broju x.

Teorem 3.5. *Ako je n prirodan broj veći od 1, nužan i dovoljan uvjet da n bude prost broj jest da za svaki cijeli broj m vrijedi*

$$\binom{m}{n} \equiv \left\lfloor \frac{m}{n} \right\rfloor \pmod{n}.$$

Dokaz. Prema teoremu 1.20, za svaki $|x| < 1$ vrijedi:

$$\begin{aligned}(1-x)^{-n-1} &= \sum_{k=0}^{\infty}\binom{-n-1}{k}(-x)^k \\ &= \sum_{k=0}^{\infty}(-1)^k\binom{n+1+k-1}{k}(-x)^k \\ &= \sum_{k=0}^{\infty}\binom{n+k}{n}x^k \\ &[k = m-n] \\ &= \sum_{m=n}^{\infty}\binom{m}{n}x^{m-n}.\end{aligned}$$

Također je

$$\begin{aligned}\sum_{m=n}^{\infty}\left\lfloor\frac{m}{n}\right\rfloor x^{m-n} &= \sum_{k=1}^{\infty}\sum_{r=0}^{n-1}\left\lfloor\frac{k\cdot n+r}{n}\right\rfloor x^{k\cdot n+r-n} \\ &= \sum_{k=1}^{\infty}\sum_{r=0}^{n-1}k\cdot x^{(k-1)n+r} \\ &= \sum_{k=1}^{\infty}\left(k\cdot x^{(k-1)n}\sum_{r=0}^{n-1}x^r\right) \\ &= (1+x+x^2+\cdots+x^{n-1})(1+2x^n+3x^{2n}+\cdots) \\ &= \frac{x^n-1}{x-1}\cdot\frac{1}{(1-x^n)^2} \\ &= \frac{1}{(1-x)(1-x^n)}\end{aligned}$$

Uočimo da je tvrdnja teorema ekvivalentna istinitosti kongruencije

$$(1-x)^{-n-1} \equiv (1-x)^{-1}(1-x^n)^{-1} \pmod{n},$$

odnosno

$$(1-x)^n \equiv 1-x^n \pmod{n}. \tag{3.1}$$

Ako je n prost broj, kongruencija vrijedi prema ranije dokazanoj lemi 2.2. U slučaju kada je n složen broj, postoji prost broj p koji je djelitelj broja n. Uspoređujući koeficijente uz x^p u (3.1) dobivamo da $n \mid \binom{n}{p}$, to jest

$$\frac{n!}{n\cdot p!\cdot(n-p)!} = \frac{(n-1)(n-2)\cdots(n-p+1)}{p(p-1)\cdots 1}$$

je cijeli broj. Dakle,

$$p \mid (n-1)(n-2)\dots(n-p+1)$$

što je u kontradikciji s pretpostavkom da je p djelitelj broja n. Zaključujemo da n ne može biti složen broj čime smo dokazali da je

$$(1-x)^n \equiv 1 - x^n \pmod{n}$$

nužan i dovoljan uvjet da n bude prost broj. □

Poglavlje 4

Generalizacije Lucasovog teorema

Od 1878. kada je Lucas ustanovio poprilično jednostavan način izračunavanja vrijednosti binomnog koeficijenta modulo prost broj, pojavile su se brojne varijacije i generalizacije navedenog teorema. U ovom poglavlju obradit ćemo dvije varijacije Lucasovog teorema za kongruencije modulo p^3, a zatim ćemo se posvetiti generalizaciji G. S. Kazandzidisa.

4.1 Varijacije Lucasovog teorema

U ovom odjeljku ćemo iskazati i dokazati dvije varijacije Lucasovog teorema za kongruencije modulo p^3, navedene u članku [1]. Za početak ćemo dokazati nekoliko tvrdnji koje su nam potrebne za bolje razumijevanje i kasnije dokazivanje teorema.

Lema 4.1. *Neka je n prirodan broj. Tada vrijedi*

$$\binom{2n}{n} = \sum_{i=0}^{n} \binom{n}{i}^2.$$

Dokaz. Raspisom identiteta

$$(1+x)^n(1+x)^n = (1+x)^{2n}$$

dobivamo jednakost

$$\left(\sum_{i=0}^{n} \binom{n}{i} x^i\right)\left(\sum_{i=0}^{n} \binom{n}{i} x^i\right) = \sum_{i=0}^{2n} \binom{2n}{i} x^i,$$

odnosno

$$\left(\binom{n}{0} + \binom{n}{1}x + \cdots \binom{n}{n}x^n\right)\left(\binom{n}{0} + \binom{n}{1}x + \cdots \binom{n}{n}x^n\right) = \sum_{i=0}^{2n} \binom{2n}{i} x^i.$$

Polinomi s lijeve i desne strane se podudaraju, pa su i koeficijenti uz x^n jednaki. Navedena činjenica nam daje jednakost

$$\binom{n}{0}\binom{n}{n} + \binom{n}{1}\binom{n}{n-1} + \cdots + \binom{n}{n}\binom{n}{0} = \binom{2n}{n}.$$

Primjenimo li svojstvo simetrije binomnih koeficijenata $\binom{m}{n} = \binom{m}{m-n}$, dobivamo

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n}^2 = \binom{2n}{n},$$

odnosno

$$\binom{2n}{n} = \sum_{i=0}^{n} \binom{n}{i}^2.$$

□

Lema 4.2. *Neka je p prost broj, $p \geq 5$. Tada vrijedi*

$$\binom{2p}{p} \equiv 2 \pmod{p^3}.$$

Dokaz. Prema prethodnoj lemi 4.1 znamo da je

$$\binom{2p}{p} = \sum_{i=0}^{p} \binom{p}{i}^2.$$

Prvi i posljedni članovi sume jednaki su 1, pa je dovoljno pokazati kako je zbroj preostalih članova kongruentan 0 modulo p^3, odnosno

$$\sum_{i=1}^{p-1} \binom{p}{i}^2 \equiv 0 \pmod{p^3}.$$

Primjenimo li svojstvo simetrije binomnih koeficijenata dobivamo

$$\sum_{i=1}^{p-1} \binom{p}{i}^2 = 2\left(\binom{p}{1}^2 + \binom{p}{2}^2 + \cdots \binom{p}{\frac{p-1}{2}}^2\right).$$

Uočimo kako je sada dovoljno pokazati

$$\binom{p}{1}^2 + \binom{p}{2}^2 + \cdots \binom{p}{\frac{p-1}{2}}^2 \equiv 0 \pmod{p^3}.$$

Ako iz lijeve strane kongruencije izlučimo p^2, dobivamo

$$p^2\left(\left(\frac{(p-1)!}{1!(p-1)!}\right)^2+\left(\frac{(p-1)!}{2!(p-2)!}\right)^2+\cdots+\left(\frac{(p-1)!}{\left(\frac{p-1}{2}\right)!\left(\frac{p+1}{2}\right)!}\right)^2\right).$$

Podijelimo li kongruenciju s p^2, preostaje pokazati

$$\left(\frac{(p-1)!}{1!(p-1)!}\right)^2+\left(\frac{(p-1)!}{2!(p-2)!}\right)^2+\cdots+\left(\frac{(p-1)!}{\left(\frac{p-1}{2}\right)!\left(\frac{p+1}{2}\right)!}\right)^2\equiv 0 \pmod{p}.$$

Uočimo da za $1\leq k\leq\frac{p-1}{2}$ vrijedi

$$\begin{aligned}\frac{(p-1)!}{k!(p-k)!} &= \frac{(p-1)(p-2)\cdots(p-k+1)}{k!}\\ &\equiv \frac{(-1)(-2)\cdots(-(k-1))}{k!}\\ &\equiv \frac{(-1)(-2)\cdots(-(k-1))}{1\cdot 2\cdots k}\\ &\equiv \pm\frac{1}{k} \pmod{p}\end{aligned}$$

pa je

$$\left(\frac{(p-1)!}{k!(p-k)!}\right)^2\equiv\left(\frac{1}{k}\right)^2\equiv l^2 \pmod{p},$$

gdje je l neki broj iz skupa

$$\left\{1,2,\ldots,\frac{p-1}{2}\right\}$$

te su različitim k-ovima pridruženi različiti l-ovi. Stoga je skup

$$\left\{\left(\frac{(p-1)!}{1!(p-1)!}\right)^2,\left(\frac{(p-1)!}{2!(p-2)!}\right)^2,\ldots,\left(\frac{(p-1)!}{\left(\frac{p-1}{2}\right)!\left(\frac{p+1}{2}\right)!}\right)^2\right\}$$

jednak skupu

$$\left\{1^2,2^2,\ldots,\left(\frac{p-1}{2}\right)^2\right\},$$

pri čemu elementi nisu nužno u istom poretku. Prema tome, imamo

$$\left(\frac{(p-1)!}{(p-1)!1!}\right)^2+\left(\frac{(p-1)!}{(p-2)!2!}\right)^2+\cdots+\left(\frac{(p-1)!}{\left(\frac{p-1}{2}\right)!\left(\frac{p+1}{2}\right)!}\right)^2\equiv 1^2+2^2+\cdots+\left(\frac{p-1}{2}\right)^2 \pmod{p}.$$

Dobiveni izraz s desne strane kongruencije je zbroj kvadrata prvih $\frac{p-1}{2}$ prirodnih brojeva. Primijenimo li formulu za sumu kvadrata prvih n prirodnih brojeva

$$\frac{n(n+1)(2n+1)}{6},$$

dobivamo

$$\frac{\frac{p-1}{2}\left(\frac{p-1}{2}+1\right)\left(2\cdot\frac{p-1}{2}+1\right)}{6} = \frac{\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)p}{6}.$$

U brojniku se nalazi faktor p pa je dobiveni izraz djeljiv s p, odnosno vrijedi

$$\frac{\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)p}{6} \equiv 0 \pmod{p}.$$

Time smo dokazali tvrdnju leme. □

Lema 4.3. *Neka su m, n i p nenegativni cijeli brojevi. Tada vrijedi*

$$\binom{(m+1)p}{n} = \sum_{i=0}^{n} \binom{mp}{n-i}\binom{p}{i}.$$

Dokaz. Raspisom identiteta

$$(1+x)^{(m+1)p} = (1+x)^{mp}(1+x)^p$$

dobivamo jednakost

$$\sum_{i=0}^{(m+1)p} \binom{(m+1)p}{i} x^i = \left(\sum_{i=0}^{mp} \binom{mp}{i} x^i\right)\left(\sum_{i=0}^{p} \binom{p}{i} x^i\right),$$

odnosno

$$\sum_{i=0}^{(m+1)p} \binom{(m+1)p}{i} x^i = \left(\binom{mp}{0} + \binom{mp}{1}x + \cdots + \binom{mp}{mp}x^{mp}\right)\left(\binom{p}{0} + \binom{p}{1}x + \cdots + \binom{p}{p}x^p\right).$$

Polinomi s lijeve i desne strane jednakosti se podudaraju, pa su i koeficijenti uz x^n jednaki. Prema tome, imamo

$$\binom{(m+1)p}{n} = \sum_{i=0}^{n} \binom{mp}{n-i}\binom{p}{i}.$$

□

Lema 4.4. *Neka je p prost broj, $p \geq 5$. Tada je*

$$\binom{np}{p} \equiv n \pmod{p^3}.$$

Dokaz. Dokaz leme provest ćemo koristeći princip matematičke indukcije po n.

Za $n = 1$ imamo

$$\binom{p}{p} = 1 \equiv 1 \pmod{p^3},$$

pa tvrdnja očito vrijedi. Za $n = 2$ tvrdnja vrijedi prema lemi 4.2. Pretpostavimo da tvrdnja $\binom{mp}{p} \equiv m \pmod{p^3}$ vrijedi za prirodne brojeve $m = 1, 2, 3, \ldots, n+1$, gdje je $n \geq 1$. Provjerimo vrijedi li tvrdnja za $m = n + 2$. Primjenom leme 4.3, imamo

$$\begin{aligned}\binom{(n+2)p}{p} &= \binom{((n+1)+1)\,p}{p} \\ &= \sum_{i=0}^{p} \binom{(n+1)p}{p-i}\binom{p}{i} \\ &= \binom{(n+1)p}{p} + \sum_{i=1}^{p-1} \binom{(n+1)p}{p-i}\binom{p}{i} + 1,\end{aligned}$$

pri čemu smo u zadnjem koraku izdvojili prvi i posljednji član sume. Primjenom pretpostavke i leme 4.3, imamo

$$\binom{(n+1)p}{p} + \sum_{i=1}^{p-1} \binom{(n+1)p}{p-i}\binom{p}{i} + 1 \equiv n + 1 + \sum_{i=1}^{p-1} \left(\binom{p}{i} \sum_{j=0}^{p-i} \binom{np}{p-i-j}\binom{p}{j} \right) + 1 \pmod{p}.$$

Preostaje nam pokazati

$$\sum_{i=1}^{p-1} \left(\binom{p}{i} \sum_{j=0}^{p-i} \binom{np}{p-i-j}\binom{p}{j} \right) \equiv 0 \pmod{p^3}.$$

Izdvojimo li iz lijeve strane kongruencije članove sume za $j = 0$ i $j = p - i$, dobivamo

$$\sum_{i=1}^{p-1} \binom{p}{i}\binom{np}{p-i} + \sum_{i=1}^{p-1} \sum_{j=1}^{p-i-1} \binom{p}{i}\binom{np}{p-i-j}\binom{p}{j} + \sum_{i=1}^{p-1} \binom{p}{i}\binom{p}{p-i}. \tag{4.1}$$

Prema Lucasovom teoremu 2.3 je svaki član srednjeg izraza u (4.1) kongruentan 0 modulo p^3 jer je

$$\binom{np}{p-i-j} \equiv \binom{n}{0}\binom{0}{p-i-j} \equiv 0 \pmod{p}, \quad 0 < p - i - j \leq p - 1,$$

$$\binom{p}{i} \equiv \binom{1}{0}\binom{0}{i} \equiv 0 \pmod{p}, \quad 0 < i \leq p-1,$$
$$\binom{p}{j} \equiv \binom{1}{0}\binom{0}{j} \equiv 0 \pmod{p}, \quad 0 < j \leq p-1.$$

Primjenimo li ponovno lemu 4.3, ostatak izraza možemo zapisati

$$\sum_{i=1}^{p-1}\binom{p}{i}\binom{np}{p-i} + \sum_{i=1}^{p-1}\binom{p}{i}\binom{p}{p-i} = \sum_{i=0}^{p}\binom{p}{i}\binom{np}{p-i} - \binom{np}{p} - 1 + \sum_{i=0}^{p}\binom{p}{i}\binom{p}{p-i} - 1 - 1$$
$$= \binom{(n+1)p}{p} - \binom{np}{p} + \binom{2p}{p} - 3.$$

Prema pretpostavci indukcije, navedeni izraz je kongruentan $(n+1) - n + 2 - 3 = 0$ modulo p^3, te smo time dokazali da vrijedi

$$\binom{(n+2)p}{p} \equiv n+2 \pmod{p^3}.$$

Prema principu matematičke indukcije zaključujemo da tvrdnja vrijedi za sve prirodne brojeve n. □

U nastavku su navedene ranije spomenute varijacije Lucasovog teorema.

Teorem 4.5. *Neka su m i n nenegativni cijeli brojevi, a p prost broj, $p \geq 5$. Tada je*

$$\binom{mp}{np} \equiv \binom{m}{n} \pmod{p^3}.$$

Dokaz. Dokaz ćemo provesti koristeći princip matematičke indukcije.

Za $n = 0$ imamo

$$1 \equiv 1 \pmod{p^3},$$

pa tvrdnja očito vrijedi. Za $n = 1$ tvrdnja vrijedi prema prethodnoj lemi 4.4.

Sada ćemo fiksirati neki $n \geq 2$ pretpostavljajući da tvrdnja vrijedi za manje n-ove te za taj n provodimo indukciju po m. Za $m < n$ imamo $\binom{mp}{np} = 0$ i $\binom{m}{n} = 0$, odnosno $0 \equiv 0 \pmod{p^3}$, pa tvrdnja očito vrijedi za svaki $m < n$. Za $m = n$ tvrdnja također očito vrijedi. Pretpostavimo da tvrdnja vrijedi za neki cijeli broj m takav da je $m \geq n$. Provjerimo vrijedi li za $m+1$. Promatramo izraz $\binom{(m+1)p}{np}$, te uvodimo oznaku $m = k+1$. Kako je $m \geq 2$, to je $k \geq 1$. Primjenom leme 4.3 dobivamo

$$\binom{(m+1)p}{np} = \sum_{i=0}^{np}\binom{mp}{np-i}\binom{p}{i}$$

$$
\begin{aligned}
&= \sum_{i=0}^{p} \binom{mp}{np-i}\binom{p}{i} \\
&= \sum_{i=0}^{p} \binom{(k+1)p}{np-i}\binom{p}{i} \\
&= \sum_{i=0}^{p} \sum_{j=0}^{np-i} \binom{kp}{np-i-j}\binom{p}{j}\binom{p}{i} \\
&= \sum_{i=0}^{p} \sum_{j=0}^{p} \binom{kp}{np-i-j}\binom{p}{j}\binom{p}{i} \\
&= \sum_{j=0}^{p} \binom{kp}{np-j}\binom{p}{j} + \sum_{i=1}^{p-1} \sum_{j=0}^{p} \binom{kp}{np-i-j}\binom{p}{j}\binom{p}{i} + \sum_{j=0}^{p} \binom{kp}{(n-1)p-j}\binom{p}{j},
\end{aligned}
$$

pri čemu smo u zadnjem koraku izdvojili članove sume za $i = 0$ i $i = p$. Primjenimo li ponovno lemu 4.3, posljednji izraz možemo zapisati

$$
\binom{(k+1)p}{np} + \sum_{i=1}^{p-1} \sum_{j=0}^{p} \binom{kp}{np-i-j}\binom{p}{j}\binom{p}{i} + \binom{(k+1)p}{(n-1)p}. \tag{4.2}
$$

Slično kao prije, korištenjem Lucasovog teorema i pretpostavke indukcije dobivamo da je svaki član srednjeg dijela izraza (4.2) kongruentan 0 modulo p^3. Ostatak jednadžbe je jednak

$$
\binom{(k+1)p}{np} + \binom{(k+1)p}{(n-1)p} \equiv \binom{k+1}{n} + \binom{k+1}{n-1} \pmod{p^3}.
$$

Uočimo da vrijedi

$$
\binom{k+1}{n} + \binom{k+1}{n-1} = \binom{k+2}{n} = \binom{m+1}{n}
$$

čime smo dokazali da je tvrdnja istinita za $m + 1$, odnosno

$$
\binom{(m+1)p}{np} \equiv \binom{m+1}{n} \pmod{p^3}.
$$

Prema principu matematičke indukcije zaključujemo da tvrdnja vrijedi za sve prirodne brojeve m i n. □

U dokazu idućeg teorema primijenit ćemo Hausnerovu metodu koju smo već koristili kod kombinatornog dokaza Lucasovog teorema.

Teorem 4.6. *Neka je p prost broj, $p \geq 5$. Neka su M, N, m_0 i n_0 nenegativni cijeli brojevi, $m_0, n_0 < p$. Tada je*

$$\binom{Mp^3 + m_0}{Np^3 + n_0} \equiv \binom{M}{N}\binom{m_0}{n_0} \pmod{p^3}.$$

Dokaz. Za početak definiramo skupove

$$A_i = \{(i, 1), (i, 2), \ldots, (i, M)\}, \quad 1 \leq i \leq p^3,$$

$$B = \{(0, 1), (0, 2), \ldots, (0, m_0)\},$$

a zatim njihovu uniju

$$A = A_1 \cup A_2 \cup \ldots \cup A_{p^3} \cup B.$$

Pri tome vrijedi $A_i = \emptyset$ ako je $M = 0$ i $B = \emptyset$ ako je $m_0 = 0$. Neka je $m = Mp^3 + m_0$. Po konstrukciji skupa A vrijedi $|A| = m$. Definiramo funkciju $f : A \to A$ koja ciklički pomiče skupove A_i, a fiksira B, to jest

$$\begin{aligned} f(i, x) &= (i + 1, x) \quad 1 \leq i \leq p^3 - 1, \\ f(p^3, x) &= (1, x), \\ f(0, x) &= (0, x). \end{aligned}$$

Prema tome, imamo

$$\begin{aligned} f(A_i) &= A_{i+1} \quad 1 \leq i \leq p^3 - 1, \\ f(A_{p^3}) &= A_1, \\ f(B) &= B. \end{aligned}$$

Funkcija f^{p^3} je identiteta na A. Sada definiramo $n = Np^3 + n_0$ i skup X kao familiju svih podskupova $C \subseteq A$ za koje je $|C| = n$. Takve skupove možemo odabrati na $\binom{m}{n}$ načina pa je $|X| = \binom{m}{n}$. Funkcija f je bijekcija, pa je $|f(C)| = |C|$. Stoga je $f : X \to X$ i vrijedi $f^{p^3} = id$. Za svaki $C \in X$ definiramo orbitu $\bar{C}$ od C kao skup $\{C, f(C), f^2(C), \ldots, f^{p^3-1}(C)\}$. Orbite particioniraju skup X, a svaka od njih sadrži točno $1, p, p^2$ ili p^3 elemenata. Označimo s X_i familiju skupova iz X čije orbite sadrže p^i elemenata. Uočimo da pritom vrijedi $|X| = |X_0| + |X_1| + |X_2| + |X_3|$. Znamo da je $|X| = \binom{m}{n} = \binom{Mp^3+m_0}{Np^3+n_0}$ te je očito $|X_3| \equiv 0 \pmod{p^3}$. Da bismo dokazali tvrdnju teorema, preostaje pokazati sljedeće

$$\begin{aligned} |X_0| &= \binom{M}{N}\binom{m_0}{n_0}, \\ |X_1| &\equiv 0 \pmod{p^3}, \\ |X_2| &\equiv 0 \pmod{p^3}. \end{aligned}$$

Promatrajmo prvo C za koji vrijedi $f(C) = C$. Svaki skup C možemo prikazati kao uniju elemenata iz A_i i B, odnosno

$$C = C_1 \cup C_2 \cup \ldots \cup C_{p^3} \cup C_0,$$

gdje je $C_i \subseteq A_i$ i $C_0 \subseteq B$. Kako je $C_0 \subseteq B$, vrijedi $f(C_0) = C_0$. Tvrdnje $f(C) = C$ i $f(C_i) \subseteq A_{i+1}$ za $1 \leq i \leq p^3 - 1$ povlače $f(C_i) = C_{i+1}$. Funkcija f je bijekcija, pa vrijedi jednakost

$$|C| = p^3|C_1| + |C_0| = n = Np^3 + n_0.$$

Iz jednakosti $|C_0| - n_0 = (N - |C_1|)p^3$ je vidljivo da p dijeli $|C_0| - n_0$. Kako je $|C_0| \leq m_0 \leq p-1$ i $n_0 \leq p-1$, slijedi $|C_0| = n_0$, a stoga je i $|C_1| = N$. Skup C_1 možemo izabrati na $\binom{M}{N}$ načina, a C_0 na $\binom{m_0}{n_0}$ različitih načina. Skup C je potpuno određen ako smo izabrali elemente od C_0 i C_1, pa primjenom principa produkta dobivamo

$$|X_0| = \binom{M}{N}\binom{m_0}{n_0},$$

čime smo dokazali prvu od tri ranije navedene tvrdnje. Preostaje pokazati $|X_1| \equiv 0 \pmod{p^3}$ i $|X_2| \equiv 0 \pmod{p^3}$.

Pretpostavimo sada da za C vrijedi $f^p(C) = C$. U tom slučaju je

$$f^p(C_1) = C_{p+1}, f^p(C_2) = C_{p+2}, \ldots, f^p(C_{p+1}) = C_{2p+1} \quad \text{itd.} \quad \text{i} \quad f(C_0) = C_0.$$

Skup C je određen ako odredimo $C_1, C_2, \ldots C_p, C_0$. Vrijedi

$$|C| = p^2|C_1| + p^2|C_2| + \cdots + p^2|C_p| + |C_0| = n = Np^3 + n_0.$$

Zaključujemo kako vrijedi $|C_0| = n_0$ i $|C_1| + |C_2| + \cdots + |C_p| = Np$. Skup C_0 možemo odabrati na $\binom{m_0}{n_0}$ načina, a $\bigcup_{i=1}^{p} C_i$ na $\binom{Mp}{Np}$ načina. Primjenimo li pravilo produkta, skup C možemo odabrati na $\binom{Mp}{Np}\binom{m_0}{n_0}$ načina. Kako su u ovaj broj uključeni i skupovi za koje vrijedi $f(C) = C$, moramo ih oduzeti od ukupnog broja. Prema tome, uz primjenu teorema 4.5, dobivamo

$$\begin{aligned} |X_1| &= \binom{Mp}{Np}\binom{m_0}{n_0} - \binom{M}{N}\binom{m_0}{n_0} \\ &= \binom{m_0}{n_0}\left(\binom{Mp}{Np} - \binom{M}{N}\right) \equiv 0 \pmod{p^3}. \end{aligned}$$

Time smo dokazali tvrdnju $|X_1| \equiv 0 \pmod{p^3}$. Preostaje dokazati da isto vrijedi za $|X_2|$.

Pretpostavimo sada da za C vrijedi $f^{p^2}(C) = C$. Analognim postupkom kao u prethodnom slučaju, zaključujemo da C možemo odabrati na $\binom{Mp^2}{Np^2}\binom{m_0}{n_0}$ načina. U taj broj uključeni

su svi skupovi C za koje vrijedi $f^p(C) = C$. Stoga moramo njih oduzeti od ukupnog broja. Tako dobivamo

$$\begin{aligned} |X_2| &= \binom{Mp^2}{Np^2}\binom{m_0}{n_0} - \binom{Mp}{Np}\binom{m_0}{n_0} \\ &= \binom{m_0}{n_0}\left(\binom{Mp^2}{Np^2} - \binom{Mp}{Np}\right) \equiv 0 \pmod{p^3}. \end{aligned}$$

Time smo pokazali da vrijedi i treća tražena tvrdnja $|X_2| \equiv 0 \pmod{p^3}$, pa je dokazana i tvrdnja teorema. □

4.2 Kazandzidisova generalizacija

Slijedi generalizacija Lucasovog rezultata koju je dao G. S. Kazandzidis, navedena u članku [10]. Za početak ćemo opisati funkcije potrebne u nastavku ovog poglavlja.

Neka je p prost broj. Tada svaki cijeli broj m možemo na jedinstven način zapisati kao $m = rp^e$, pri čemu $p \nmid r$, odnosno $p^e \parallel m$. Funkcija E daje eksponent najveće potencije prostog broja p koja dijeli zadani broj m, to jest

$$E(m) = e.$$

Funkcija F daje klasu ostataka p-slobodnog dijela zadanog broja m, to jest

$$F(m) \equiv r \equiv \frac{m}{p^{E(m)}} \pmod{p}.$$

Dodatno, definiramo $E(0) = \infty$ i $F(0) = 0$.

U nastavku, zbog jednostavnosti zapisujemo $E\binom{m}{n}$ i $F\binom{m}{n}$ umjesto $E(\binom{m}{n})$ i $F(\binom{m}{n})$ te koristimo sljedeće oznake prikaza brojeva m, n i $m - n$ u bazi p:

$$\begin{aligned} m &= \sum m_i p^i, \\ n &= \sum n_i p^i, \\ m - n &= \sum a_i p^i, \end{aligned}$$

gdje svuda sumiramo po i.

Kazandzidis je dao sljedeće proširenje Lucasovog teorema

$$\binom{m}{n} \equiv (-p)^{E\binom{m}{n}} \prod \frac{m_i!}{n_i! a_i!} \pmod{p^{E\binom{m}{n}+1}}$$

koje primjenom teorema 1.14 i dijeljenjem s $p^{E\binom{m}{n}}$ te korištenjem dosadašnjih oznaka možemo zapisati

$$F\binom{m}{n} \equiv (-1)^{E\binom{m}{n}} \prod \frac{m_i!}{n_i! a_i!} \pmod{p}.$$

U nastavku ćemo $F\binom{m}{n}$ odrediti pomoću $E(m!)$, $F(m!)$ i $E\binom{m}{n}$. Vrijednosti ovih funkcija su rezultati koje su redom dali A. M. Legendre, L. Stickelberger i E. Kummer. U sljedećoj propoziciji navedena su osnovna svojstva funkcija E i F potrebna u daljnjem radu.

Propozicija 4.7. *Funkcije E i F zadovoljavaju sljedeća svojstva:*

a) $F(m) \equiv 0 \pmod{p}$ *ako i samo ako je* $m = 0$.

Dokaz. Za $m = 0$ je po definiciji $F(m) = 0$. Ako je $m \neq 0$, onda iz zapisa $m = rp^e$ možemo izlučiti p^e te nam ostaje p-slobodni dio $r \neq 0$ koji nije djeljiv s p. Prema tome je $F(m) \not\equiv 0 \pmod{p}$, pa zaključujemo da tvrdnja $F(m) \equiv 0 \pmod{p}$ vrijedi samo ako je $m = 0$. □

b) $E(p^e) = e$; $F(p^e) \equiv 1 \pmod{p}$.

Dokaz. Očito vrijedi $p^e \parallel p^e$ iz čega slijedi $E(p^e) = e$.
Iz $\dfrac{p^e}{p^e} = 1$ slijedi tvrdnja $F(p^e) \equiv 1 \pmod{p}$. □

c) $m \equiv F(m)p^{E(m)} \pmod{p^{E(m)+1}}$.

Dokaz. Uočimo kako su obje strane kongruencije djeljive s $p^{E(m)}$. Kada izraz podijelimo s $p^{E(m)}$ prema teoremu 1.14 dobivamo ekvivalentnu jednakost $F(m) \equiv F(m) \pmod{p}$ koja je očito istinita. □

d) $m_i = 0$ *za* $0 \leq i < E(m)$; $m_{E(m)} \equiv F(m) \pmod{p}$.

Dokaz. Najveća potencija od p koja dijeli m je po definiciji p^e, gdje je $e = E(m)$. Kada razvijamo broj m u bazi p, prema teoremu 1.6 dijelimo m s p, pri čemu je prvih $E(m)$ puta ostatak 0. U zapisu broja m u bazi p te znamenke su jednake 0, odnosno $m_i = 0$ za $0 \leq i < E(m)$. Prema tome, m možemo zapisati u obliku

$$m = 0 \cdot p^0 + 0 \cdot p^1 + \ldots + 0 \cdot p^{E(m)-1} + m_{E(m)} p^{E(m)} + m_{E(m)+1} p^{E(m)+1} + \ldots m_k p^k.$$

Ako iz navedenog zapisa izlučimo najveću potenciju broja p, dobivamo

$$m = p^{E(m)}(m_{E(m)} + m_{E(m)+1} p + \ldots + m_k p^{k-E(m)}),$$

odakle slijedi $m_{E(m)} \equiv F(m) \pmod{p}$. □

e) $E(m)$ je potpuno aditivna funkcija, to jest $E(mn) = E(m) + E(n)$.

Dokaz. Neka su m i n cijeli brojevi koje možemo zapisati u obliku $m = r_1 p^{e_1}$ i $n = r_2 p^{e_2}$, gdje je p prost broj te vrijedi $p \nmid r_1$ i $p \nmid r_2$. Njihovim umnoškom dobivamo

$$m \cdot n = r_1 p^{e_1} \cdot r_2 p^{e_2} = r_1 r_2 \cdot p^{e_1+e_2}.$$

Kako p ne dijeli r_1 i r_2, tada prema teoremu 1.8 ne dijeli niti njihov umnožak $r_1 r_2$. Uočimo kako je najveća potencija broja p koja dijeli $m \cdot n$ upravo $p^{e_1+e_2}$, odnosno vrijedi tvrdnja $E(mn) = E(m) + E(n)$. □

f) $F(m)$ je potpuno multiplikativna funckija, to jest $F(mn) = F(m) \cdot F(n)$.

Dokaz. Neka su m i n cijeli brojevi koje možemo zapisati u obliku $m = r_1 p^{e_1}$ i $n = r_2 p^{e_2}$ gdje je p prost broj te vrijedi $p \nmid r_1$ i $p \nmid r_2$. Njihovim umnoškom dobivamo

$$m \cdot n = r_1 p^{e_1} \cdot r_2 p^{e_2} = r_1 r_2 \cdot p^{e_1+e_2}.$$

Kako p ne dijeli r_1 i r_2, tada prema teoremu 1.8 ne dijeli niti njihov umnožak $r_1 r_2$. Uočimo kako je p-slobodni dio od mn jednak $r_1 r_2$, odnosno vrijedi tvrdnja $F(mn) = F(m) \cdot F(n)$. □

g) Ako je $k > E(m)$, onda za svaki cijeli broj a vrijedi

$$E(m + ap^k) = E(m) \quad i$$

$$F(m + ap^k) \equiv F(m) \pmod{p}.$$

Dokaz. Po definiciji imamo

$$m + ap^k = F(m)p^{E(m)} + ap^k = p^{E(m)}(F(m) + ap^{k-E(m)}),$$

pri čemu smo izlučili najveću potenciju od p, a to je zbog uvjeta $k > E(m)$ upravo $p^{E(m)}$. Uočimo kako je $k - E(m)$ veće od 0, pa je $ap^{k-E(m)}$ djeljivo s p. Znamo da $F(m)$ nije djeljivo s p, pa tada niti zbroj $F(m) + ap^{k-E(m)}$ nije djeljiv s p. Prema tome slijedi tvrdnja

$$E(m + ap^k) = E(m).$$

Uočimo kako je $F(m + ap^k) = F(m) + ap^{k-E(m)}$, pa uz činjenicu da p dijeli $ap^{k-E(m)}$, slijedi tvrdnja

$$F(m + ap^k) \equiv F(m) \pmod{p}.$$

□

h) Ako $p \nmid m$*, onda je* $E(m) = 0$ *i* $F(m) \equiv m \pmod{p}$.

Dokaz. Ako $p \nmid m$, onda je p^0 najveća potencija broja p koja dijeli m, pa vrijedi tvrdnja $E(m) = 0$.

Ako $p \nmid m$, onda kad iz broja m izlučimo najveću potenciju broja p koja dijeli m, to jest izlučimo p^0, ostaje nam $m = 1 \cdot m$, pa slijedi $F(m) \equiv m \pmod{p}$. □

i) $E(1) = 0$*;* $F(1) \equiv 1 \pmod{p}$.

Dokaz. Niti jedan prost broj p ne dijeli 1, pa je ovo specijalni slučaj prethodne tvrdnje. Uvrstimo li $m = 1$ dobivamo $E(1) = 0$ i $F(1) \equiv 1 \pmod{p}$. □

j) Za svaki cijeli broj a *vrijedi* $F(ap^e) \equiv F(a) \pmod{p}$.

Dokaz. Neka je $a = sp^t$, gdje $p \nmid s$. Tada je očito $F(ap^e) \equiv F(a) \equiv s \pmod{p}$. □

Nakon što smo iskazali i dokazali svojstva funkcija E i F potrebna za daljnje tvrdnje i izvod generalizacije, slijedi dio u kojem izračunavamo vrijednosti od $E(p^k!)$ i $F(p^k!)$.

Teorem 4.8. *Za* $k \geq 1$ *imamo*

$$E(p^k!) = p^{k-1} + E(p^{k-1}!) \quad i$$

$$F(p^k!) \equiv -F(p^{k-1}!) \pmod{p}.$$

Dokaz. Izraz $p^k!$ možemo zapisati kao

$$p^k! = 1 \cdot 2 \cdots (p-1)(p \cdot 1)(p+1) \cdots (2p-1)(p \cdot 2)(2p+1) \cdots (p^k - 1)(p \cdot p^{k-1}).$$

Želimo li odrediti $E(p^k!)$ potrebno je promatrati članove produkta koji sadrže potencije od p. Uz primjenu svojstva potpune aditivnosti funkcije E dobivamo

$$\begin{aligned} E(p^k!) &= E((p \cdot 1)(p \cdot 2) \cdots (p \cdot p^{k-1})) \\ &= E(p^{p^{k-1}} \cdot (1 \cdot 2 \cdots p^{k-1})) \\ &= E(p^{p^{k-1}} \cdot p^{k-1}!) \\ &= E(p^{p^{k-1}}) + E(p^{k-1}!) \\ &= p^{k-1} + E(p^{k-1}!). \end{aligned}$$

Koristeći svojstvo potpune multiplikativnosti funkcije F i teorem 1.15 imamo

$$F(p^k!) = F(1 \cdot 2 \cdots (p-1)(p \cdot 1)(p+1) \cdots (2p-1)(p \cdot 2)(2p+1) \cdots (p^k - 1)(p \cdot p^{k-1}))$$

$$
\begin{aligned}
&= F(1 \cdot 2 \cdots (p-1)(p+1) \cdots (2p-1)(2p+1) \cdots (p^k-1)(p \cdot 1)(p \cdot 2) \cdots (p \cdot p^{k-1})) \\
&= F(1) \cdot F(2) \cdots F(p-1)F(p+1) \cdots F(2p-1)F(2p+1) \cdots \\
&\qquad \cdots F(p^k-1)F((p \cdot 1)(p \cdot 2) \cdots (p \cdot p^{k-1})) \\
&\equiv 1 \cdots (p-1)(p+1) \cdots (2p-1)(2p+1) \cdots (p^k-1) \cdot F(p^{p^{k-1}} \cdot p^{k-1}!) \\
&\equiv (-1)^{p^{k-1}} F(p^{k-1}!) \pmod{p}.
\end{aligned}
$$

Broj p je ili neparan ili jednak 2 pa vrijedi

$$(-1)^{p^{k-1}} \equiv -1 \pmod{p}.$$

Iz navedenog slijedi tvrdnja

$$F(p^k!) \equiv -F(p^{k-1}!) \pmod{p}.$$

□

Pomoću ovog teorema rekurzivno smanjujemo eksponent u potenciji broja p. On nam omogućuje da uzastopnim ponavljanjem nakon konačno mnogo koraka izračunamo najveću potenciju od p koja dijeli $p^k!$ odnosno p-slobodni dio od $p^k!$.

Korolar 4.9. *Vrijedi*

$$E(p^k!) = \frac{p^k - 1}{p - 1} \quad i$$

$$F(p^k!) \equiv (-1)^k \equiv (-1)^{E(p^k!)} \pmod{p}.$$

Dokaz. Uzastopnom primjenom teorema 4.8, dobivamo:

$$
\begin{aligned}
E(p^k!) &= p^{k-1} + E(p^{k-1}!) \\
&= p^{k-1} + p^{k-2} + E(p^{k-2}!) \\
&\vdots \\
&= p^{k-1} + p^{k-2} + \cdots + p^1 + E(p^1!) \\
&= p^{k-1} + p^{k-2} + \cdots + p^1 + p^0 + E(p^0!) \\
&= p^{k-1} + p^{k-2} + \cdots + p + 1
\end{aligned}
$$

Uočimo da smo dobili geometrijski niz od k članova, pri čemu je prvi član niza 1, a kvocijent p. Primijenimo li formulu za sumu geometrijskog niza, dobivamo

$$E(p^k!) = \frac{p^k - 1}{p - 1}.$$

Uzastopnom primjenom teorema 4.8, dobivamo

$$\begin{aligned} F(p^k!) &\equiv -F(p^{k-1}!) \\ &\equiv (-1)^2 F(p^{k-2}!) \\ &\vdots \\ &\equiv (-1)^k F(1) \\ &\equiv (-1)^k \pmod{p} \end{aligned}$$

Dakle, vrijedi tvrdnja $F(p^k!) \equiv (-1)^k \pmod{p}$. Primijetimo da je

$$E(p^k!) = 1 + p + \cdots + p^{k-1} \equiv k \pmod{2}$$

za p neparan, pa je

$$F(p^k!) \equiv (-1)^{E(p^k!)} \pmod{p}.$$

□

Teorem 4.10. *Neka je $m+1, m+2, \ldots, m+p^k$ niz od p^k uzastopnih cijelih brojeva, te P njihov produkt. Postoji jedinstven j_0, $1 \leq j_0 \leq p^k$ takav da $p^k \mid m+j_0$. Neka je $m+j_0 = ap^k$, pri čemu p može biti djelitelj od a. Tada je*

$$E(P) = E(a) + E(p^k!) \quad i$$

$$F(P) = F(a)F(p^k!).$$

Dokaz. Za $j > j_0$ imamo $m + j = ap^k + (j - j_0)$. Prema propoziciji 4.7(g) je

$$E(m+j) = E(ap^k + (j-j_0)) = E(j-j_0) \quad \text{i}$$

$$F(m+j) = F(ap^k + (j-j_0)) \equiv F(j-j_0) \pmod{p},$$

pri čemu je

$$j - j_0 \in \{1, 2, \ldots, p^k - j_0\}.$$

Za $j < j_0$ imamo $m + j = (a-1)p^k + (p^k - (j_0 - j))$. Uočimo kako je $j_0 - j$ veće od 0, pa je $p^k - (j_0 - j)$ manje od p^k. Sada možemo kao u prethodnom slučaju, primijeniti svojstvo iz propozicije 4.7(g), a prema njemu vrijedi

$$E(m+j) = E((a-1)p^k + (p^k - (j_0 - j))) = E(p^k - (j_0 - j)) \quad \text{i}$$

$$F(m+j) = F((a-1)p^k + (p^k - (j_0 - j))) \equiv F(p^k - (j_0 - j)) \pmod{p},$$

pri čemu je

$$p^k - (j_0 - j) \in \{p^k - 1, p^k - 2, \ldots, p^k - j_0 + 1\}.$$

Ovime smo pokazali da svi elementi osim ap^k koji je djeljiv s p^k, imaju u nekom poretku iste eksponente i ostatke kao brojevi od 1 do p^k. Za ap^k znamo da vrijedi $E(ap^k) = E(a) + E(p^k)$ i $F(ap^k) = F(a)F(p^k)$. Iz navedenog slijedi

$$E(P) = E(1 \cdot 2 \cdots (p^k - 1) \cdot ap^k) = E(a) + E(p^k!) \quad \text{i}$$

$$F(P) = F(1 \cdot 2 \cdots (p^k - 1) \cdot ap^k) = F(a)F(p^k!).$$

□

U nastavku ćemo odrediti vrijednost od $E(m!)$ i $F(m!)$ pomoću tvrdnji koje smo dosad dokazali.

Korolar 4.11. *Neka je $m = ap^k$. Tada je*

$$E(m!) = aE(p^k!) + E(a!) \quad i$$

$$F(m!) \equiv F(a!)F(p^k!)^a \equiv (-1)^{ka}F(a!) \pmod{p}.$$

Dokaz. Imamo

$$\begin{aligned} m! &= (ap^k)! \\ &= (1 \cdots p^k) \cdot ((p^k + 1) \cdots (2p^k)) \cdots (((a-1)p^k + 1) \cdots (ap^k)). \end{aligned}$$

Uočimo kako ovdje imamo a nizova od p^k uzastopnih cijelih brojeva. Primjenimo li teorem 4.10 za svaki od a nizova brojeva pri čemu je m redom jednak $0, p^k, \ldots, (a-1)p^k$, dobivamo

$$\begin{aligned} E(m!) &= E((1 \cdots p^k) \cdot ((p^k + 1) \cdots (2p^k)) \cdots (((a-1)p^k + 1) \cdots (ap^k))) \\ &= E(1 \cdots p^k) + E((p^k + 1) \cdots (2p^k)) + \cdots + E(((a-1)p^k + 1) \cdots (ap^k)) \\ &= E(1) + E(p^k!) + E(2) + E(p^k!) + \cdots + E(a) + E((p^k)!) \\ &= aE(p^k!) + E(1 \cdot 2 \cdots a) \\ &= aE(p^k!) + E(a!), \end{aligned}$$

$$\begin{aligned} F(m!) &\equiv F((1 \cdots p^k) \cdot ((p^k + 1) \cdots (2p^k)) \cdots (((a-1)p^k + 1) \cdots (ap^k))) \\ &\equiv F(1 \cdots p^k) \cdot F(((p^k + 1) \cdots (2p^k)) \cdots F(((a-1)p^k + 1) \cdots (ap^k))) \\ &\equiv F(1)F(p^k!)F(2)F(p^k!) \cdots F(a)F(p^k!) \\ &\equiv (p^k!)^a F(1 \cdot 2 \cdots a) \\ &\equiv F(p^k!)^a F(a!) \\ &\equiv (-1)^{ka}F(a!) \pmod{p}, \end{aligned}$$

pri čemu smo u zadnjem koraku primijenili korolar 4.9. □

Specijalni slučaj prethodnog korolara, kad je a manji od p, daje sljedeću tvrdnju.

Korolar 4.12. *Neka je $m = ap^k$, $0 \leq a < p$. Tada je*

$$E(m!) = aE(p^k!) \quad i$$

$$F(m!) \equiv (-1)^{ka} a! \equiv (-1)^{E(m!)} a! \pmod{p}.$$

Dokaz. Primjenom korolara 4.11 i činjenice da je $0 \leq a < p$, imamo

$$\begin{aligned} E(m!) &= aE(p^k!) + E(a!) \\ &= aE(p^k!), \end{aligned}$$

$$\begin{aligned} F(m!) &\equiv (-1)^{ka} F(a!) \\ &\equiv (-1)^{ka} a! \\ &\equiv (-1)^{E(m!)} a! \pmod{p}. \end{aligned}$$

□

Teorem 4.13. *Neka je $m = ap^k + m^*, 0 \leq m^* < p$. Tada je*

$$E(m!) = E((ap^k)!) + E(m^*!) = aE(p^k!) + E(a!) + E(m^*!) \quad i$$

$$F(m!) \equiv F((ap^k)!) \cdot F(m^*) \equiv (-1)^{ka} F(a!) F(m^*!) \pmod{p}.$$

Dokaz. Za izraz $m!$ vrijedi

$$\begin{aligned} m! &= (ap^k + m^*)! \\ &= 1 \cdot 2 \cdots (ap^k)(ap^k + 1) \cdots (ap^k + m^*) \\ &= (ap^k)!(ap^k + 1) \cdots (ap^k + m^*) \end{aligned}$$

Primjenom korolara 4.11 i svojstva potpune aditivnosti funkcije E, imamo:

$$\begin{aligned} E(m!) &= E((ap^k)!(ap^k + 1) \cdots (ap^k + m^*)) \\ &= E((ap^k)!) + E(ap^k + 1) + \cdots + E(ap^k + m^*) \\ &= aE(p^k!) + E(a!) + E(1) + \cdots + E(m^*) \\ &= aE(p^k!) + E(a!) + E(m^*!), \end{aligned}$$

Primjenom korolara 4.11 i svojstva potpune multiplikativnosti funkcije F, imamo:

$$F(m!) \equiv F((ap^k)!(ap^k + 1) \cdots (ap^k + m^*))$$

$$\begin{aligned}
&\equiv F((ap^k)!)F(ap^k+1)\cdots F(ap^k+m^*)\\
&\equiv F((ap^k)!)F(1)\cdots F(m^*)\\
&\equiv F((ap^k)!)F(m^*!)\\
&\equiv (-1)^{ka}F(a!)F(m^*!) \pmod{p}.
\end{aligned}$$

□

Specijalni slučaj prethodnog teorema, kad je a manji od p, daje idući rezultat.

Korolar 4.14. *Neka je $m = ap^k + m^*$, $0 \le m^* < p^k$, $0 \le a < p$. Tada je*

$$E(m!) = aE(p^k!) + E(m^*!) \quad i$$

$$F(m!) \equiv (-1)^{ka}a!F(m^*!) \equiv (-1)^{aE(p^k!)}a!F(m^*!) \pmod{p}.$$

Dokaz. Primjenom teorema 4.13 i činjenice da je $0 \le a < p$, imamo

$$\begin{aligned}
E(m!) &= E((ap^k + m^*)!)\\
&= aE(p^k!) + E(a!) + E(m^*!)\\
&= aE(p^k!) + E(m^*!),
\end{aligned}$$

$$\begin{aligned}
F(m!) &\equiv F((ap^k + m^*)!)\\
&\equiv (-1)^{ka}F(a!)F(m^*!)\\
&\equiv (-1)^{ka}a!F(m^*!)\\
&\equiv (-1)^{aE(p^k!)}a!F(m^*!) \pmod{p}.
\end{aligned}$$

□

U sljedećem teoremu navest ćemo rezultate za $E(m!)$ i $F(m!)$ koje su dobili A. M. Legendre i L. Stickelberger.

Teorem 4.15. *Neka je $m = \sum m_i p^i$, pri čemu je $0 \le m_i < p$. Tada je*

$$E(m!) = \sum m_i \frac{p^i - 1}{p-1} = \frac{m - \sum m_i}{p-1} \quad i$$

$$F(m!) \equiv (-1)^{\sum im_i} \prod (m_i!) \equiv (-1)^{E(m!)} \prod (m_i!) \pmod{p}$$

Dokaz. Neka je k najmanji cijeli broj za koji je $p^{k+1} > m$. Neka je $m^* = m - m_k p^k$. Tada je $m = m_k p^k + m^*$, pri čemu je $0 \leq m_k < p$ i $0 \leq m^* < p^k$. Uzastopnom primjenom korolara 4.14, dobivamo

$$\begin{aligned} E(m!) &= E((m_k p^k + m^*)!) \\ &= m_k E(p^k!) + E(m^*!) \\ &\vdots \\ &= m_k E(p^k!) + m_{k-1} E(p^{k-1}!) + \cdots + m_0 E(p^0!) \\ &= \sum m_i \frac{p^i - 1}{p - 1} \\ &= \frac{m - \sum m_i}{p - 1}. \end{aligned}$$

Uzastopnom primjenom korolara 4.14, dobivamo

$$\begin{aligned} F(m!) &\equiv F((m_k p^k + m^*)!) \\ &\equiv (-1)^{k m_k} m_k! F(m^*!) \\ &\equiv (-1)^{k m_k} m_k! (-1)^{(k-1) m_{k-1}} m_{k-1}! \cdots \\ &\equiv (-1)^{\sum i m_i} \prod m_i! \\ &\equiv (-1)^{\sum m_i \frac{p^i - 1}{p-1}} \prod m_i! \\ &\equiv (-1)^{E(m!)} \prod m_i! \pmod{p}. \end{aligned}$$

□

U nastavku ćemo navesti rezultat E. Kummera za $E\binom{m}{n}$ te konačno, generalizaciju Lucasovog teorema, tj. Kazandzidisov rezultat za $F\binom{m}{n}$.

Korolar 4.16. *Neka su za cijele brojeve m i n takve da je* $0 \leq n \leq m$

$$m = \sum m_i p^i, \qquad n = \sum n_i p^i, \qquad m - n = \sum a_i p^i$$

prikazi brojeva m, n i m − n u bazi p. Tada vrijedi

$$E\binom{m}{n} = \sum \frac{n_i + a_i - m_i}{p - 1} \quad i$$

$$F\binom{m}{n} \equiv (-1)^{E\binom{m}{n}} \prod \frac{m_i!}{n_i! a_i!} \pmod{p}$$

Dokaz. Uz primjenu svojstva potpune aditivnosti funkcije E i potpune multiplikativnosti funkcije F, tvrdnje slijede direktno iz teorema 4.15. □

Bibliografija

[1] D.F. Bailey, *Two p^3 variations of Lucas' theorem*, Journal of Number Theory 35 (1990.), 208-215.

[2] L.E. Clarke, E.M. Wright, *Problem 4704*, The American Mathematical Monthly, Vol. 64, No. 8 (1957.), 597-598.

[3] A. Dujella, *Uvod u teoriju brojeva*, dostupno na `http://e.math.hr/zeta/utblink.pdf` (lipanj 2018.)

[4] N. J. Fine, *Binomial Coefficients Modulo a Prime*, The American Mathematical Monthly, Vol. 54, No 10, Part 1 (1947.), 589-592.

[5] A. Granville, *Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers*, Organic mathematics (Burnaby, BC, 1995), 253-276. CMS Conf. Proc. 20, American Mathematical Society Providence, 1997.

[6] M. Hausner, *Applications of a Simple Counting Technique*, The American Mathematical Monthly, Vol. 90, No. 2 (1983.), 127-129.

[7] V. Krčadinac, *Osnove algoritama*, dostupno na `https://web.math.pmf.unizg.hr/ nastava/oa/oa-skripta.pdf` (lipanj 2018.)

[8] R. Nowlan, *Édouard Lucas*, dostupno na `http://www.robertnowlan.com/pdfs/Lucas,%20Edouard.pdf` (svibanj 2018.)

[9] B. Pavković, D. Veljan, *Elementarna matematika II*, Školska knjiga, Zagreb 1995.

[10] D. Singmaster, *Notes on binomial coefficients. I–A generalization of Lucas' congruence*, J. London Math. Soc. (2) 8 (1974.), 545-548.

[11] D. Veljan, *Kombinatorna i diskretna matemtika*, Algoritam, Zagreb 2001.

Sažetak

Francuski matematičar Édouard Lucas ustanovio je 1878. jednostavnu metodu izračunavanja vrijednosti binomnog koeficijenta $\binom{m}{n}$ modulo prost broj p pomoću znamenaka zapisa prirodnih brojeva m i n u bazi p. Jedan od iskaza Lucasovog teorema glasi: Ako su $m = m_k p^k + m_{k-1} p^{k-1} + \cdots + m_1 p + m_0$ i $n = n_k p^k + n_{k-1} p^{k-1} + \cdots + n_1 p + n_0$ zapisi nenegativnih cijelih brojeva m i n u bazi p, gdje je p prost broj, onda je

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \pmod{p}.$$

Ovaj diplomski rad podijeljen je na četiri poglavlja. U prvom poglavlju navodimo osnovne pojmove i tvrdnje potrebne za razumijevanje nastavka rada. U drugom poglavlju navodimo iskaz Lucasovog teorema, a zatim ga dokazujemo na algebarski i kombinatorni način. U trećem poglavlju prikazujemo neke primjene Lucasovog teorema, dok je posljednje poglavlje posvećeno generalizacijama.

Summary

French mathematician Édouard Lucas established in 1878 a simple method of computing binomial coefficient $\binom{m}{n}$ modulo a prime number p using the digits of base p representation of integers m and n. One statement of Lucas' theorem is the following. If $m = m_k p^k + m_{k-1} p^{k-1} + \cdots + m_1 p + m_0$ and $n = n_k p^k + n_{k-1} p^{k-1} + \cdots + n_1 p + n_0$ are expansions of non-negative integers m and n in base p, where p is a prime, then

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \pmod{p}.$$

This graduate thesis is divided into four chapters. In the first one we introduce basic terms and claims necessary to understand the rest of the thesis. In the second chapter we present the statement of Lucas' theorem and then we prove it algebraically and combinatorially. In the third chapter we present some applications of Lucas' theorem, while the last chapter is devoted to its generalizations.

Životopis

Rođena sam 10.12.1993. u Varaždinu. Pohađala sam *IV.* OŠ Varaždin do 2008. godine, a zatim nastavila školovanje na Drugoj gimnaziji Varaždin, opći smjer. Usporedno s obveznim školovanjem, pohađala sam školu stranih jezika Žiger gdje sam učila engleski jezik. U srpnju 2012. godine, nakon završetka gimnazije, upisala sam studij matematike, nastavnički smjer na Prirodoslovno-matematičkom fakultetu u Zagrebu. Godine 2016. završila sam preddiplomski studij te nastavila obrazovanje na diplomskom studiju matematike, nastavnički smjer na istom fakultetu. Tijekom fakultetskog obrazovanja više puta sam sudjelovala na Danima otvorenih vrata Prirodoslovno-matematičkog fakulteta te Večerima matematike u organizaciji Hrvatskog matematičkog društva.